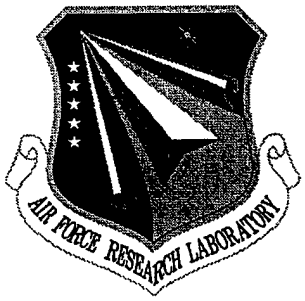
AFRL-IF-RS-TR-1998-55
Final Technical Report
April 1998



HIGH ASSURANCE SECURE X.500

Secure Computing Corporation

Cornelia Murphy, Dick O'Brien, and Dan Thomsen

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-SN-RS-TR-1998-55 has been reviewed and is approved for publication.

APPROVED: Mary L. Denz

MARY L. DENZ
Project Engineer

FOR THE DIRECTOR:

WARREN H. DEBANY, JR., Technical Advisor
Information Grid Division
Information Directorate

If your address has changed or if you wish to be removed from the Air Force Research Laboratory Rome Research Site mailing list, or if the addressee is no longer employed by your organization, please notify AFRL/IFGB, 525 Brooks Road, Rome, NY 13441-4505. This will assist us in maintaining a current mailing list.

Do not return copies of this report unless contractual obligations or notices on a specific document require that it be returned.

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	April 1998	Final May 96 - Dec 97

4. TITLE AND SUBTITLE

HIGH ASSURANCE SECURE X.500

5. FUNDING NUMBERS

C - F30602-96-C-0065
PE - 33140F
PR - 7820
TA - 04
WU - 32

6. AUTHOR(S)

Cornelia Murphy, Dick O'Brien, and Dan Thomsen

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Secure Computing Corporation
2675 Long Lake Road
Roseville MN 55113

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AFRL/IFGB
525 Brooks Road
Rome NY 13441-4505

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

AFRL-IF-RS-TR-1998-55

11. SUPPLEMENTARY NOTES

AFRL Project Engineer: Mary L. Denz/IFGB/(315) 330-2030

12a. DISTRIBUTION AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This is the final report for the High Assurance Secure (HAS) X.500 program. It summarizes progress made on development of a high assurance, Multilevel Secure X.500 network directory server. The program was to develop an important enabling technology for building secure integrated network applications. Upon completion, the HAS X.500 system would have lowered operational costs and increased productivity by providing a high assurance networked database management system (DBMS) on the Secure Network Server LOCK 6 platform allowing connectivity between databases on networks at different classification levels and sharing of directory information between levels. The program consisted of four major components: porting a trusted DBMS to a high assurance platform, porting an X.500 Directory Server Agent to a high assurance platform, developing a relational directory information base, and coordinating and sharing progress with the security community. A majority of the DBMS port was completed prior to a redirection of the Defense Message System program which prompted an early termination for this program.

14. SUBJECT TERMS

Computer Security, Trusted Database Management, X.500, Network Connectivity

15. NUMBER OF PAGES

20

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Contents

List of Figures

Section 1

Introduction

1.1 Identification

This document is the final technical report for the project *High Assurance Secure X.500* completed under contract number F30602-96-C-0065 for Rome Laboratory.

1.2 Program Overview

1.2.1 Objectives

The original objective of this work was to design and prototype a high assurance, Multilevel Secure (MLS) X.500 network directory server as illustrated in Figure 1-1. The resulting system was to provide protection of both multilevel and unclassified but sensitive, X.500 directory information across local and wide area networks. The system was also to include integrated Fortezza cryptography, attribute level labelling, and a networked relational Database Management System (DBMS) interface for maintenance and developing custom database applications.

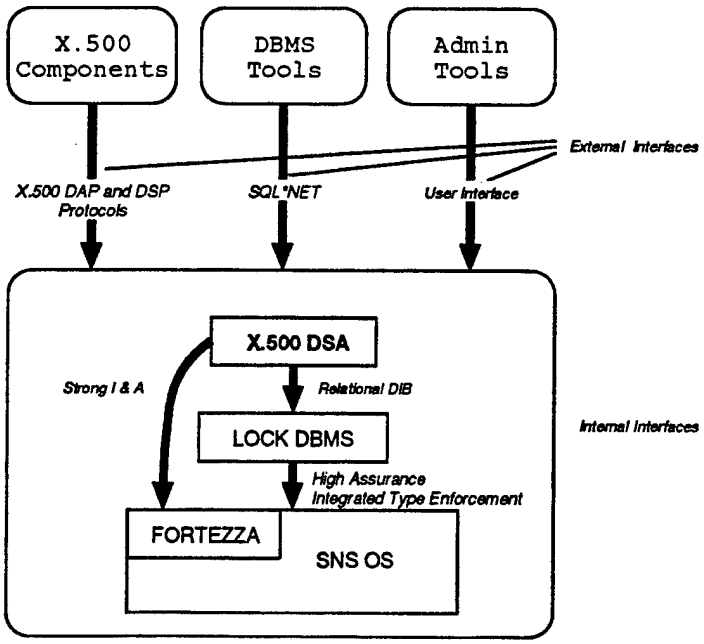


Figure 1-1: High Assurance Secure X.500 System

1.2.2 Approach Summary

Development of a high assurance, secure X.500 system was originally based on the latest release of the X.500 software maintained and distributed by the ISODE Consortium (IC) and on the latest release of Trusted Oracle V7.

The IC software was to be enhanced so that a relational DBMS could be used to implement the Directory Information Base (DIB). SCC originally planned to use SRI and their Computer Science Laboratory (CSL) as a consultant to help develop the requirements and design for a generic relational database implementation of the DIB. This work was to be based on work SRI has done on an initial read-only MLS X.500 prototype using Trusted Oracle.

To develop a high assurance, secure X.500, the Directory System Agent (DSA) code and protocols were to be implemented on the high assurance SNS LOCK 6 platform[1], and a relational DIB was to be implemented using the modified IC code and Trusted Oracle V7 on the SNS LOCK 6 platform. The FORTEZZA cryptographic functionality was to be integrated with the system to provide FORTEZZA based X.509 authentication. A network connection to Trusted Oracle on SNS LOCK 6 would be included to allow easy maintenance and initialization of the DIB and to support more sophisticated relational DBMS queries against the DIB. Finally, an MLS version of X.500 was to be developed that provides for the labelling of individual attributes of an entry in the DIB and that allows for chaining between DSAs at different levels.

An initial prototype was to be demonstrated half way through the program. The initial prototype was to consist of the LOCK DBMS [2] prototype

1. upgraded to the SNS LOCK 6 platform,
2. upgraded to the latest Trusted Oracle release, and
3. enhanced with network connectivity capabilities.

A final high assurance, full X.500 prototype was to be demonstrated at program completion. For the final prototype, the initial prototype functionality was to be enhanced to support

1. modified ISODE Consortium object code that implements a complete MLS X.500 directory server using a relational database for the directory,
2. a generic relational implementation of the DIB,
3. SQL tools for maintenance and complicated searching of the DIB, and
4. strong X.509 standard based identification and authentication by integrating FORTEZZA card cryptography.

In addition, the program was to publicize results of the program through conference papers and participation in X.500 Birds of a Feather meetings.

1.2.3 Results Summary

A majority of the work on the HAS X.500 program was in porting Trusted Oracle version 7.2 to the LOCK 6 platform. LOCK 6 was an enhancement of the SNS providing a POSIX interface. Support for LOCK 6 development and assurance work was withdrawn by the government before the platform could be completed. Once LOCK 6 development was cancelled, it unfortunately followed that the HAS X.500 program be terminated since the LOCK 6 platform was critical in reaching HAS X.500 objectives.

[1] Development initiated by Maryland Procurement Office, contract number MDA904-93-C-C034

[2] Developed for Rome Laboratory under contract number F30602-C-92-0094.

Following is a summary of what was accomplished in the abbreviated HAS X.500 program.

1. Enhanced LOCK DBMS
   - Software Requirement Specification [3]
   - Software Design Document [2]
   - Trusted Oracle Version 7.2 port to SNS LOCK 6 platform accessible through SQL*DBA
2. X.500 Directory Service
   - The IC DSA port was abandoned to take advantage of the SNS LOCK 6 contract modification to include porting the Unisys DSA.
   - The need for a C++ compiler was identified as an issue since it was not available on the SNS LOCK 6 platform.
   - Switching from the IC DSA to the Unisys DSA eliminated the need for the SRI subcontract and substantially reduced this task from one that developed a Relational DIB to one that made the HAS X.500 system interoperate with an existing Relational DIB.
   - No work was performed on the port of the DSA before the program was terminated.
3. Technology Transfer
   - A conference paper entitled "Incremental Assurance for Multilevel Applications" [4] was written and presented at the 1997 Annual Computer Security Applications Conference. The paper describes an approach, incremental assurance, for balancing security with the economic pressures of developing secure systems. The approach combines many of the existing techniques for reducing costs in developing secure systems. The paper illustrates incremental assurance with three example applications involving high assurance and multilevel DBMS technology.
   - The port of ORACLE to the LOCK 6 platform while the platform was still in development provided the HAS X.500 program the opportuinty to
     (a) influence development of the platform to include features required to support a large commercial application, the ORACLE server, and
     (b) serve as an operational testbed for the platform as the large ORACLE server exercised the limitations of the platform.

1.3 Document Overview

The report is structured as follows:

- Section 1, **Introduction**, provides an overview of the document.
- Section 2, **Enhanced LOCK DBMS**, discusses progress that was made in porting Trusted Oracle to the SNS LOCK 6 platform.
- Section 3, **X.500 Directory Service** , discusses progress that was made in porting the X.500 DSA to the SNS LOCK 6 platform.
- Section 4, **Summary**, includes a summary of the results and observations of the project along with lessons learned and suggestions for future work.

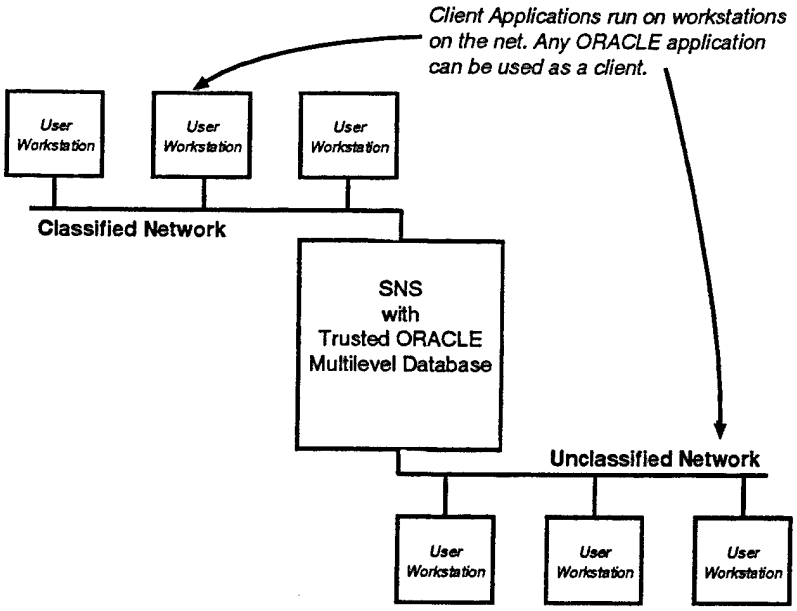


Figure 2-2: Network LOCK DBMS

Section 2 Enhanced LOCK DBMS

Under this task, Secure Computing's high assurance LOCK DBMS prototype [1] was to be enhanced by moving it to the SNS LOCK6 platform and adding network connectivity. The resulting configuration is illustrated in Figure 2-2. The network LOCK DBMS system would allow Oracle client applications running on network workstations to access highly secure, and possibly multilevel, databases on the SNS LOCK 6 platform.

For the X.500 system, network access to the database would allow the DIB database managers to perform many of their functions remotely over the network. The initial relational DIB scripts could be created via tools running on their workstation. It would also be possible to move relational DIB implementations easily from one system to another by exporting them from one system and importing them to the other via the standard RDBMS export and import functions. Maintenance on the DIB database could be done using standard RDBMS tools.

The Network LOCK DBMS was also to provide a means for sophisticated database applications, developed on the user workstations, to process the data in the DIB to obtain information that might not be easily obtained via standard Directory User Agent (DUA) commands. For example, a user would be able to correlate information about different users easily.

A Network LOCK DBMS system would have significant uses beyond being the basis for the secure X.500 DIB. Some proposed uses were

- storage of cryptographic keys and digital signatures,

- central clearing house for integrating legacy systems operating at different security levels, and
- quick development environment for multilevel applications.

Work on the HAS X.500 program focused on the Enhanced LOCK DBMS task and was able to complete the following.

- Software Requirement Specification [3]
- Software Design Document [2]
- Trusted Oracle Version 7.2 port to SNS LOCK 6 platform accessible through SQLDBA

Work remaining to be done on the Enhanced LOCK DBMS task included completing SQLNet connectivity and performing and documenting testing.

Section 3

X.500 Directory Service

The X.500 Directory Service component of the program was to develop full support for X.500 capabilities, including support for strong authentication as defined in X.509, and a relational DIB using the Enhanced LOCK DBMS prototype. Originally, the approach was to

1. replace the IC code DIB with a relational implementation,
2. port the modified IC software to the SNS LOCK 6 platform,
3. port the ISODE protocol stack to the SNS LOCK 6 platform, and
4. add strong authentication between DUA and DSA based on FORTEZZA.

Prior to beginning any of the work, near term plans for future development on the SNS LOCK 6 platform were changed to include porting the Unisys DSA to the platform. The HAS X.500 program moved to a Unisys DSA for several reasons both technical and economical in nature.

- The Unisys DSA design was more modular and better lent itself to being integrated with Type Enforcment. This strengthened the assurability of the implementation and reduced costs for type enforcing the DSA.
- The Unisys X.400 DSA already had an interface to a relational database reducing the effort from developing a Relational DIB to engineering the HAS X.500 system to interoperate with an existing Relational DIB.
- Settling on a single DSA increased synergy between HAS X.500 and SNS LOCK 6.
- The SNS LOCK 6 solution also included a reclassifier which would provide further cost advantage since it provided functionality to be implemented in the Multi-Chaining Option.

One disadvantage in using IC code was losing the ability to hand the modified DSA code to the Consortium for distribution with future releases of their system.

Before much work was done on the port of the DSA, the need for an SNS LOCK 6 platform based C++ compiler was identified. There were no plans to port a C++ compiler to the LOCK 6 platform. A search was made for alternative DSAs. Before the HAS X.500 program was terminated the following alternatives were considered.

1. University of Michigan LDAP Code
   - written in C
   - supports LDAP
   - no licensing fees
   - no relational database interface
   - does not connect to X.500 without a gateway (LDAPD)
   - would be a type of proxy not real X.500 server
2. Datacraft
   - written in C
   - support DAP and LDAP
   - $300K in licensing fees
   - provides a relational interface to Oracle

- Datacraft claims an international patent on any relational database interface to X.500 server

No additional work on the task was done due to the lack of a supported SNS LOCK 6 system. Work remaining to be done on the X.500 Directory Server task included identifying and porting a suitable DSA.

Section 4

Summary

4.1 Lessons

During the execution of the program, several conclusions were reached and lessons learned that should be considered for any future work that my result from the HAS X.500 program.

C++ Compiler for the X.500 DSA Both the ISODE Consortium and Unisys X.500 DSAs required a C++ Compiler on the SNS LOCK 6 platform. A C++ compiler was not available, and would not be available in the short term, on the SNS LOCK 6 platform. When searching for optional X.500 DSAs, the Datacraft DSA is the only implementation found that did not require a C++ compiler. Unfortunately, the cost of obtaining the source for the DSA was prohibitive.

Risk of relying on other projects currently under development This project was terminated before completion because support for the LOCK 6 platform, on which our work was to be done, was withdrawn by the government. As a result we did not have a stable platform on which to continue our work. The lesson learned is that a program's risk is substantially increased when the program needs positive results from another ongoing development that has its own risks.

4.2 Future Work

The following list identifies potential areas for future work.

Incremental Assurance There is a great deal of work necessary to turn incremental assurance into a methodology for reducing the costs of developing high assurance systems. One idea that may reduce costs is a taxonomy of security architectures and how they can be used for incremental assurance. For example, the firewall model fits well with incremental assurance, because it incorporates the security into a single component. That component can be improved/replaced as time goes on. Another idea might be the description of security components that can be used as building blocks in incremental assurance.

Resurrect HAS X.500 Development of the basic LOCK 6 platform has transitioned to the Boeing Military Airplanes Division F-22 Operational Flight Program Build System contract number P.C. HT4411. HAS X.500 development could resume on the Boeing LOCK 6 platform once this platform becomes stable and the appropriate assurance work is done on it.

Bibliography

[1] Secure Computing Corporation. "Final Report for the LOCK DBMS Program". LOCK DBMS CDRL A015, Secure Computing Corporation, 2675 Long Lake Road, Roseville, Minnesota 55113-2536, 1996.

[2] Secure Computing Corporation. "Software Design Document for the High Assurance Secure X.500 System". HAS X.500 CDRL A007, Secure Computing Corporation, 2675 Long Lake Road, Roseville, Minnesota 55113-2536, 1996.

[3] Secure Computing Corporation. "Software Requirements Specification for the High Assurance Secure X.500 System". HAS X.500 CDRL A006, Secure Computing Corporation, 2675 Long Lake Road, Roseville, Minnesota 55113-2536, 1996.

[4] D.J. Thomsen and M. Denz. Incremental Assurance for Multilevel Applications. In *Proceedings of the 13th Computer Security Applications Conference*, pages ?–?, December 1997.